Concept Paper # 256

Presented to the Department of Administrative Services (DAS)
Date Prepared:

Name of document to be reviewed:

Security Information Event Management (SIEM) Consolidation

(Please check one item listed in the following two sections)

Document for review and approval:

__ **Request for Proposal (RFP)**
__ **Request for Service (RFS)**
__ **Request for Quote (RFQ)**
__ **Invitation to Qualify**
__ **Sole Source Procurement**
X **Statement of Work**
__ **Staff Augmentation**
__ **Master Agreement Purchase**

Document for review only:

__ **Master Agreement**
__ **Request for Information (RFI)**

Agency: ___Department of Administrative Services

RFP Reference #: RFP not required, State of Iowa, IDR already owns and operates the product.

Projected cost over $50,000? Yes _X__ No ___
Projected agency staff hours over 750? Yes _X__ No _ __

Project Cost, Funds and Funding Source:

Total project cost is estimate between $200K–350K non-inclusive of current staff expense. Funding for this project will come from a combination of sources. The ISO will contribute $32,000 that would normally go toward annual license of the SPLUNK log search product. SPLUNK will be de-commissioned after EventTracker is rolled out. The Iowa Department of Revenue will contribute $40,000 that they had budgeted to go for SIEM. The Department of Human Services has committed to assist with partial funding. The Iowa Department of Transportation has also expressed interest in this project although funding and/or amount is not confirmed. The remainder of the cost and ongoing expenses will be assessed to agencies as part of a utility fee or shared services expense. Additional

funding is being requested through Enterprise IT consolidation funds or other agency sources.

EventTracker Enterprise Site License	$ 280,000
Hardware and Networking Services	$ 50,000
Total	$ 320,000

Internal Resources/Costs: ITE Technical Support / 1 FTE / ITS5 = $ 100,000

External Resources/Costs:

EventTracker Professional Services	$ 124,900
EventTracker annual M&S	$ 56,000

Timelines:

Purchase EventTracker Enterprise license	July 2013
Purchase Hardware	July 2013
Begin phased SIEM pilot rollout	Aug 2013
Vendor rollout of SIEM	Sept 2013
Customization of reporting	Nov 2013
Completed phased roll out of pilot agencies	Feb 2013
Enterprise-wide coverage	Dec 2014

* IDR funds need to be spent in this fiscal year.

Goal:

This proposal is to expand the SIEM project to more comprehensively collect, analyze and report log data, increasing the number and coverage of the devices providing input. The goal will be to collect information from all participating and as many non-participating agencies as possible.

SIEM systems are critical when attempting sort through millions of log events in order to be alerted to an incident and with the subsequent investigation. These devices are also extremely useful on for day to day operational use.

DOT, DHS, DAS, IDR and many other state agencies have federal requirements mandating log collection and correlation.

Background:

In FY09 the State of Iowa piloted its first SIEM project. Driven by funding shortfalls a piecemeal combination of open source software and commercial products were implemented. In 2010 the Department of Revenue implemented a comprehensive commercial SIEM solution in order to comply with IRS audit requirements. The SIEM system chosen by IDR is in use by numerous fortune 100 companies and several Federal agencies. The EventTracker SIEM system is a true enterprise class SIEM system

correlating log results, managing USB device auditing and providing File Integrity Monitoring and alerting upon changes.

Expected Results:

What are the tangible and intangible benefits of this purchase for this agency and/or state government?

- Compliance with Federal requirements
- Early incident detection
- Operational troubleshooting tools
- Statewide consolidation to one single SIEM system
- Additional reporting and alerting services
- USB device management, monitoring and reporting
- File Integrality Monitoring – Alerts when important files change
- Proven system currently in use in IDR
- Current staff expertise on installing and operating the system
- Virtually unlimited log capacity with the addition of commodity hardware

Can these benefits be quantified in financial terms? If yes, please explain.

Yes. We are investing money into this solution to reduce the likelihood of a data breach and the associated costs. Some of these direct costs can include regulatory fines, litigation expenses, citizen notification, identity theft services, call center support and reduced employee productivity. Recently the State of South Carolina experienced a data breach costing over 30 million dollars to remediate. The implementation of a SIEM alone would not prevent such a breach but it will mitigate the risk and reduce the cost associated to a breach by early detection. Other costs include the disruption of critical services and the associated public backlash. Many agencies within the Executive branch have some type of audit requirement. This system will fulfill audit requirements or most if not all agencies.

How will you be more effective as a result of this purchase?

Currently DAS/ITE maintains a costly and cumbersome SIEM system that only has the capacity to deal with log files and alert based on a preset pattern match. Implementing the EventTracker SIEM system will allow the enterprise to process billions of log messages, monitor USB drive usage, alert on file changes, correlate alerts based on IDS notifications and Anti-Virus alerts. The goal of any SIEM system is to distill a variety of information into actionable items.

How will service to your customers be enhanced as a result of this purchase?

This solution will satisfy regulatory compliance audit requirements. Effective use of a SIEM system will reduce risk to the state networks and the data they contain. It has been shown that effective use of a SIEM system can reduce security incident investigation time by over 75%. Operational incident response benefits even more from SIEM systems when it

comes to troubleshooting an issue affecting the network. The current logging solution in place has no monitoring component after normal business hours. The EventTracker SIEM solution offers a 24/7 monitoring service (for a fee) that can alert the appropriate staff about issues.

Testing and Acceptance:

The Iowa Department of Revenue has this system in place today. IDR has been operational with the EventTracker system for 3 + years. Recently the ISO used the IDR EventTracker system to rule out the possibility of malicious activity inside the IDR network. The ability to quickly assess and make a decision about a potential security issue allowed the operations team narrow their scope and resolve the issue in a much timelier manner.

Some of the Interested Parties:

This is an Enterprise level project. The scope of this project will be all participating agencies and as many non-participating agencies as are willing to participate.

Some of the Recipients of this Service:

State of Iowa Agencies

Standards:

The system is compliant with enterprise standards.

Architecture:

The architecture of this system is a common "hub and spoke" type architecture. There is a centrally managed web based console. Information can be fed to the central server(s) directly by hosts or in larger instances a collection point serer can be placed in an agencies network to collect and forward data. With the Enterprise license an unlimited number of forwarders can be deployed. The backend collection and correlation capacity can be expanded by simply adding more severs to form a SIEM cluster.

Business Continuity / Disaster Recovery:

This product will support BC and DR activities and planning.

Recommendations from the State CIO:

NOTE: *Where applicable, all DAS GSE Procurement and IA Administrative Code 11-105 and 11-106 requirements and procedures are to be followed. Reference: http://das.gse.iowa.gov/procurement/, specifically: http://das.gse.iowa.gov/procurement/adminrules/.*

Duplication recommendation from the State CIO to the DAS Director:

a) Is there duplication within Government? *(Please identify duplication at the agency level, as well as within the enterprise)*
b) Can an existing program be modified to address a new need?
c) Do you have any similar program in existence?
d) Have you sought IT procurements for similar programs in the past?
e) Do you have purchasing documents for similar programs?
f) Do you have similar purchasing documents that could be used as a starting point for this program?
g) Is there anything you could provide that could assist the agency with this IT procurement?
h) Are there alternatives available to the agencies?

Recommendation of the State CIO to the DAS Director:

Authorize this IT procurement Yes _X_ No ___
Alternatives suggested by the State CIO (see comments below) Yes ___ No _X_

Additional comments from the State CIO:

TEC recommends to the State CIO that ITE proceed to find an enterprise solution. The concept is supported but funding is uncertain. Subsequently approved by the CIO.

DAS Director's action:
Authorize this IT procurement Yes _X_ No ___

DAS Director's signature and date:

The above IT procurement concept approved by Director Carroll on __5/1/13__

Comments: **None.**